REMARKS

Claims 1-30 were examined and reported in the Office Action. Claims 1-30 are rejected. Claims 22-23, 25 and 29 are canceled. Claims 1, 4, 7, 12, 17, 21, 24 and 28 are amended. Claims 1-21, 24, 26-28 and 30 remain.

Applicant requests reconsideration of the application in view of the following remarks.

I.   35 U.S.C. §103

A.   It is asserted in the Office Action that claims 1-3, 7-11, and 17-23 are rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent No. 5,956,407 issued to Slavin ("Slavin"), in view of U. S. Patent 5,933,501 issued to Leppek ("Leppek"). Applicant respectfully traverses the aforementioned rejection for the following reasons.

According to MPEP §2142 "[t]o establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure." (In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). Further, according to MPEP §2143.03, "[t]o establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. (In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)." "*All words in a claim must be considered* in judging the patentability of that claim against the prior art." (In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970), emphasis added.)

Applicant's amended claim 1 contains the limitations of "... a key generating section, the key generating section to generate a plurality of individual keys based on a main key, each of said plurality of individual keys is different from one another; a decryption generating section coupled to the key generating section and a main decryption section, the decryption generating section to generate a plurality of individual decryption processes based on the main decryption section and the plurality of individual keys, each of said plurality of individual decryption processes is different from one another; and a main encryption section, the main encryption section using the main key to encrypt content, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption processes, and each of the plurality of decryption processes and its respective individual key can decrypt content encrypted by the main encryption section."

Applicant's amended claim 7 contains the limitations of "... generating a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another; generating a plurality of individual decryption processes based on a main decryption process and the plurality of individual keys, each of said plurality of individual decryption processes being different from one another; and encrypting content based on an encryption process and the main key, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption processes, and each of the plurality of decryption processes and its respective individual key can decrypt content encrypted by the encryption process."

Applicant's amended claim 17 contains the limitations of "[a] program storage device readable by a machine comprising instructions that cause the machine to: generate a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another; generate a plurality of individual decryption processes based on a main decryption process and the plurality of individual keys, each of said plurality of individual decryption processes being different from one another; and encrypt content based on an encryption process and the main key."

Applicant's amended claim 21 contains the limitations of "generate a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another; generate a plurality of individual decryption processes based on a main decryption process and the plurality of individual keys, each of said plurality of individual decryption processes being different from one another; and encrypt content based on an encryption process and the main key, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption processes, and each of the plurality of decryption processes and its respective individual key can decrypt content encrypted by the encryption process."

That is, users each have a different decryption process for decrypting content encrypted with the encryption process. Each of the differing decryption processes has individual keys.

Slavin discloses a method for encrypted communication where messages are created and public keys are looked up for a recipient. The message is encoded by a first process using a first portion of the public key to generate an intermediate encoded message. Then a second encoding process uses a second portion of the public key to generate the final encoded message. The final encoded message is sent to a recipient. "To decode the message, the receiver has created a decoding key as a function of the prime factors used to create the encoding key." (Slavin, column 6, lines 31-34). That is, each recipient uses the same decoding process and different decoding keys. Slavin does not teach, disclose or suggest "the decryption generating section to generate a plurality of individual decryption processes based on the main decryption section and the plurality of individual keys, each of said plurality of individual decryption processes is different from one another; and a main encryption section, the main encryption section using the main key to encrypt content, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption processes, and each of the plurality of decryption processes and its respective individual key can decrypt content encrypted by the main encryption section."

Leppek discloses a "virtual" encryption method that uses a sequence of encryptor operators to form a compound encryption operator. Leppek further discloses that "the data processing scheme of the present invention is effectively a `virtual` encryption and decryption scheme, as it does not actually perform any encrypting of the data, but rather assembles selected ones of a plurality of true encryption mechanisms into a cascaded sequence of successively different encryption operators." (Leppek, column 4, lines 48-59). It is asserted in the Office Action that Leppek discloses "a system that generates a plurality of individual decryption processes wherein each decryption process is different from one another." (Office Action, page 5, second paragraph). Applicant respectfully disagrees. Leppek simply uses decryption operators from a decryption operator database to decrypt the stream that was virtually encrypted with a sequence of encryptor operators. Leppek does not teach, disclose or suggest "the decryption generating section to generate a plurality of individual decryption processes based on the main decryption section and the plurality of individual keys, each of said plurality of individual decryption processes is different from one another; and a main encryption section, the main encryption section using the main key to encrypt content, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of decryption processes, and each of the plurality of decryption processes and its respective individual key can decrypt content encrypted by the main encryption section."

Therefore, neither Slavin, Leppek, nor the combination of the two teach, disclose or suggest the limitations contained in Applicant's amended claims 1, 7, 17 and 21, as listed above. Since neither Slavin, Leppek, nor the combination of the two teach, disclose or suggest all the limitations of Applicant's amended claims 1, 7, 17 and 21 there would not be any motivation to arrive at Applicant's claimed invention. Thus, Applicant's amended claims 1, 7, 17 and 21 are not obvious over Slavin in view of Leppek since a *prima facie* case of obviousness has not been met under MPEP §2142. Additionally, the claims that directly or indirectly depend from amended claims 1, 7, 17 and 21, namely claims 2-3, 8-11, 18-20, and 22-23, respectively, would also not be obvious over Slavin in view of Leppek for the same reason.

Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejections for Claims 1-3, 7-11 and 17-23 are respectfully requested.

B. It is asserted in the Office Action that claims 4-6, 12-16, and 24-30 are rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent No. 5,720m034 issued to Case ("Case"), in view of Leppek and further in view of U. S. Patent 4,503,287 issued to Morris et al ("Morris"). Applicant respectfully traverses the aforementioned rejection for the following reasons.

Applicant's amended claim 4 contains the limitations of "... a key generating section, the key generating section to generate a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another; an encryption generating section coupled to the key generating section and a main encryption section, the encryption generating section to generate a plurality of individual encryption processes based on the main encryption section and the plurality of individual keys, each of said plurality of individual encryption processes being different from one another; and a main decryption section, the main decryption section using the main key to decrypt cypher-content, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt content to be decrypted by the main decryption section."

Applicant's amended claim 12 contains the limitations of "... generating a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another; generating a plurality of individual encryption processes based on a main encryption process and the plurality of individual keys, each of said plurality of individual encryption processes being different from one another; and decrypting cypher-content based on a main decryption process and the main key, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt cipher-content to be decrypted by the main decryption process."

Applicant's amended claim 24 contains the limitations of "... generate a plurality of individual keys based on a main key, each of said plurality of individual keys being different from one another; generate a plurality of individual encryption processes based on a main encryption process and the plurality of individual keys, each of said plurality of individual decryption processes being different from one another; and decrypt cypher-content based on a main decryption process and the main key, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt cypher-content to be decrypted by the main decryption process."

Applicant's amended claim 28 contains the limitations of "distribute a plurality of individual keys to a plurality of customers, each of said plurality of individual keys being different from one another; distribute a plurality of individual encryption processes to the plurality of customers, each of said plurality of individual decryption processes being different from one another; and receive cypher-content from the plurality of customers, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt cypher-content to be decrypted by a main decryption process."

Applicant has discussed Leppek above. Similarly as discussed above, Leppek does not teach, disclose or suggest "an encryption generating section coupled to the key generating section and a main encryption section, the encryption generating section to generate a plurality of individual encryption processes based on the main encryption section and the plurality of individual keys, each of said plurality of individual encryption processes being different from one another" or "distribute a plurality of individual encryption processes to the plurality of customers, each of said plurality of individual decryption processes being different from one another; and receive cypher-content from the plurality of customers, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective

individual key can encrypt cypher-content to be decrypted by a main decryption process."

It is asserted in the Office Action that since Case discloses a message is encoded using a slave key that the slave key would change the encoding process every time. Applicant respectfully traverses this assertion. Case discloses the encoding process (i.e. algorithm) that encodes a message does not change with a slave key. The message changes by using a slave key. Applicant asserts that the assertion in the Office Action is broadly using the term "process" for encoding, i.e., all of the steps to perform encoding. Applicant, however, uses the term "process" as a separate encryption entity, such as a computer program, a function, etc. In other words, Applicant's claimed invention generates and distributes distinct encoding means that can only be used by the intended recipient. Case does not teach, disclose or suggest "an encryption generating section coupled to the key generating section and a main encryption section, the encryption generating section to generate a plurality of individual encryption processes based on the main encryption section and the plurality of individual keys, each of said plurality of individual encryption processes being different from one another" or "distribute a plurality of individual encryption processes to the plurality of customers, each of said plurality of individual decryption processes being different from one another; and receive cypher-content from the plurality of customers, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt cypher-content to be decrypted by a main decryption process."

Morris is relied on for disclosing the Master key is used to decipher the session encryptor key, which is transmitted as cipher text. (Office Action, page 8, second paragraph). Morris, however, does not teach, disclose or suggest "an encryption generating section coupled to the key generating section and a main encryption section, the encryption generating section to generate a plurality of individual encryption processes based on the main encryption section and the plurality of individual keys, each of said plurality of individual encryption processes being different from one

another" or "distribute a plurality of individual encryption processes to the plurality of customers, each of said plurality of individual decryption processes being different from one another; and receive cypher-content from the plurality of customers, wherein only a one of the plurality of individual keys is used in conjunction with only a one of the plurality of encryption processes, and each of the plurality of encryption processes and its respective individual key can encrypt cypher-content to be decrypted by a main decryption process."

Therefore, even if the inventions of Leppek, Case and Morris were combined, the resulting invention would still not teach, disclose or suggest Applicant's claimed limitations in claims 4, 12, 24 and 28. Since Case, Morris, or the combination of the two do not teach, disclose or suggest all the limitations of Applicant's amended claims 4, 12, 24 and 28, as listed above, there would not be any motivation to arrive at Applicant's claimed invention. Thus, Applicant's amended claims 4, 12, 24 and 28 are not obvious over Leppek and Case in view of Morris since a *prima facie* case of obviousness has not been met under MPEP §2142. Additionally, the claims that directly or indirectly depend from amended claims 4, 12, 24 and 28, namely claims 5-6, 13-16, 25-27, and 29-39, respectively, would also not be obvious over Leppek and Case in view of Morris for the same reason.

Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejections for Claims 4-6, 12-16 and 24-30 are respectfully requested.
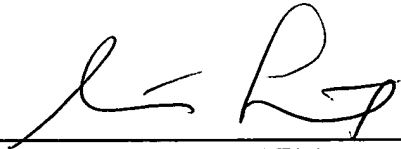
CONCLUSION

In view of the foregoing, it is believed that all claims now pending, namely 1-21, 24, 26-28 and 30, patentably define the subject invention over the prior art of record and are in condition for allowance and such action is earnestly solicited at the earliest possible date.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly extension of time fees.

Respectfully submitted,

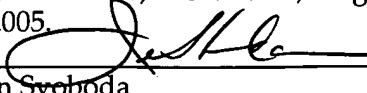BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

Dated: March 1, 2005   By: _____

Steven Laut, Reg. No. 47,736

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail with sufficient postage in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P. O. Box 1450, Alexandria, Virginia 22313-1450 on March 1, 2005.

_____
Jean Svoboda